

REMARKS

Claim Rejections - 35 USC §103

The examiner rejected claims 1-5, 7, 9, 11-17 and 26 under 35 USC §103(a) as unpatentable over Alonso et al. (6,434,700) in view of Jackson, Trevor European Patent Application No. 0911738. The applicant respectfully disagrees.

Claim 1 has been amended to incorporate the limitations recited in claims 2, 7 and 10 (claims 2, 7 and 10 have been canceled). The rejection of claim 1 should be withdrawn for at least the reasons set forth below regarding the rejection of claim 10.

The rejection of claims 2, 3, 4, 5, 7, 9 and 11, should be withdrawn for at least the reasons set forth below.

Claim 12 recites a computer network comprising a plurality of interconnected network devices including a disk drive connected to an authentication server, wherein the disk drive comprises an interface for receiving from a client computer a user ID and a user access request to access a network device, and for transmitting device access data to the client computer.

Alonso does not disclose or suggest these limitations. In the first paragraph on page 3 of the office action, the examiner concedes that Alonso teaches a conventional access control server (ACS) for generating and transmitting the device access data to a client computer. Therefore, the examiner is incorrect in asserting (on page 7 of the office action) that Alonso discloses a disk drive comprising an interface for receiving from a client computer a user ID and a user access request to access a network device, and for transmitting device access data to the client computer. In Alonso, these operations are performed by the CPU within the ACS and not by the disk controller of the disk drive.

Further, nothing in Jackson would suggest to implement these operations within a disk drive. The rejection should therefore be withdrawn.

The rejection of claims 13, 14, 15, 16, and 17 should be withdrawn for at least the reasons set forth above.

Claim Rejections - 35 USC §103

The examiner rejected claims 6, 8, 10, and 18-26 under 35 USC §103(a) as unpatentable over Alonso in view of Jackson and further in view of DeTreville (6,609,199). The applicant respectfully disagrees.

Claim 1 has been amended to incorporate the limitations recited in claims 2, 7 and 10 (claims 2, 7 and 10 have been canceled). As amended, claim 1 recites that the user access data comprises a plurality of user identifiers and corresponding access rights to the plurality of network devices, the disk stores encrypted device access data associated with the network devices, the device access data for use in authenticating device access requests transmitted from client computers to the network devices, and the encrypted device access data is stored on the disk during manufacture of the disk drive.

In rejecting claim 10, the examiner asserts that DeTreville discloses to store encrypted access data on a disk during manufacture of a disk drive. This rejection is incorrect for at least two reasons. First, DeTreville discloses to manufacture a CPU, not a disk drive. Second, DeTreville discloses to manufacture a CPU with a pair of public and private keys 150 that are unique to the CPU (col. 5, lines 54-55). That is, the public and private keys are for accessing the CPU and not other devices connected to a network. Nowhere does DeTreville disclose or suggest to store encrypted device access data on the disk during manufacture of a disk drive, wherein the device access data for use in

authenticating device access requests transmitted from client computers to the network devices. The rejection should be withdrawn.

Claim 22 recites a disk drive comprising an interface for receiving an encrypted device access request and for inputting/outputting user data from/to a client computer. The disk drive further comprises an internal drive key and an encrypted secret device key shared with an authentication server. Cryptographic circuitry in the disk drive decrypts the encrypted secret device key using the internal drive key to generate a decrypted secret device key. The disk drive comprises an authenticator for authenticating the device access request using the decrypted secret device key.

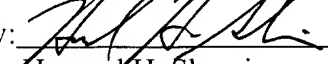
The examiner asserts that because Jackson and DeTreville teach the use of a secret device key, the authorization access server (ACS) disclosed by Alonso could be modified to include a secret device key for use in authenticating a device access request. However, modifying Alonso in view of Jackson and DeTreville would result in an authentication server implementing network authentication facilities using a secret device key and not a disk drive implementing network authentication facilities using a secret device key. The rejection should therefore be withdrawn.

The rejection of the remaining claims should be withdrawn for at least the reasons set forth above.

CONCLUSION

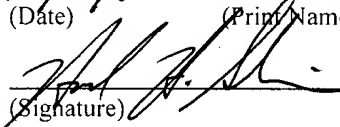
The above amendments to the claims do not add new matter or raise new issues; the applicant respectfully requests the examiner enter the amendments. In view of the foregoing amendments and remarks, the rejections under 35 USC §102 and §103 should be withdrawn. The examiner is encouraged to contact the undersigned over the telephone in order to resolve any remaining issues that may prevent the immediate allowance of the present application.

Respectfully submitted,

Date: 12/30/05 By: 
Howard H. Sheerin
Reg. No. 37,938
Tel. No. (303) 765-1689

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on:

12/30/05 Howard H. Sheerin
(Date) (Print Name)

(Signature)